(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年9 月30 日 (30.09.2004)

PCT

(10) 国際公開番号
WO 2004/084071 A1

(51) 国際特許分類[7]: G06F 11/00

(21) 国際出願番号: PCT/JP2004/003533

(22) 国際出願日: 2004 年3 月17 日 (17.03.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-072372 2003 年3 月17 日 (17.03.2003) JP

(71) 出願人 (米国を除く全ての指定国について): セイコーエプソン株式会社 (SEIKO EPSON CORPORATION) [JP/JP]; 〒1630811 東京都新宿区西新宿二丁目4番1号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 黒田 直人 (KURODA, Naoto) [JP/JP]; 〒3928502 長野県諏訪市大和三丁目3番5号 セイコーエプソン株式会社内 Nagano (JP).

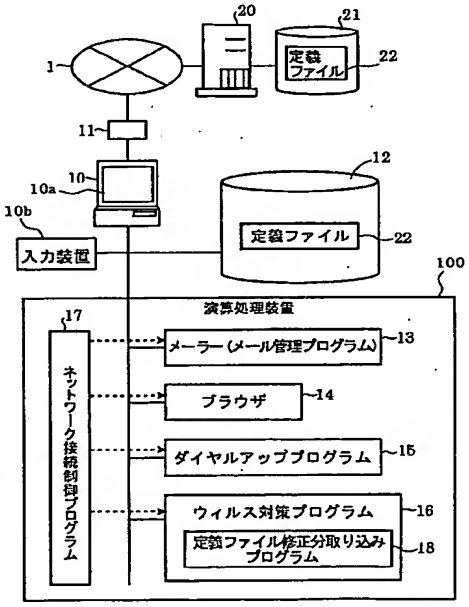
(74) 代理人: 特許業務法人 湘洋内外特許事務所 (THE PATENT CORPORATE BODY SHOWYOU INTERNATIONAL); 〒2200004 神奈川県横浜市西区北幸二丁目9-10 横浜HSビル7階 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: METHOD AND SYSTEM FOR ACQUIRING PARTICULAR DATA UPON START OF A PARTICULAR PROGRAM

(54) 発明の名称: 特定のプログラムの起動時に、特定のデータを取得する方法およびシステム



22...DEFINITION FILE
10b...INPUT DEVICE
22...DEFINITION FILE
17...NETWORK CONNECTION CONTROL PROGRAM
100...COMPUTER DEVICE
13...MAILER (MAIL MANAGEMENT PROGRAM)
14...BROWSER
15...DIAL-UP PROGRAM
16...VIRUS-COUNTERMEASURE PROGRAM
18...DEFINITION FILE CORRECTION ACQUISITION PROGRAM

(57) Abstract: A computer device (100) executing a network control program (17) detects a start instruction for a mailer (13) or a browser (14). Upon detection of the start instruction, a dial-up program (15) is started and a network connection is established, so that a definition file correction acquisition program (18) is started and a definition file correction is acquired from a server (20). After this, the mailer (13) or the browser (14) which is instructed to start is started.

(57) 要約: ネットワーク制御プログラム（１７）を実行する演算処理装置（１００）は、メーラー（１３）およびブラウザ（１４）のいずれかについての起動指示の検知を行う。起動指示を検知すると、ダイヤルアッププログラム（１５）を起動してネットワーク接続を確立し、定義ファイル修正分取り込みプログラム（１８）を起動して、サーバ２０から定義ファイル修正分を取り込む。この後、起動が指示されたメーラー（１３）およびブラウザ（１４）のいずれかについての起動を行う。

WO 2004/084071 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

特定のプログラムの起動時に、特定のデータを取得する方法およびシステム

技術分野

本発明は、特定のプログラムの起動時に、ネットワークを介して特定のデータを取得する技術に係り、特に、コンピュータのネットワークセキュリティ強化に用いられるデータの取得に利用可能な技術に関する。

背景技術

コンピュータウィルスに対する対策のためにコンピュータにインストールされたウィルス対策ソフトウェアは、通常、コンピュータを起動したときに、ウィルス対策ソフトウェアも立ち上がる。そして、コンピュータをネットワークに接続すると、一定時間おきにネットワークを通じて所定のサーバに接続し、サーバに蓄積されているウィルス定義ファイルから、修正分を取り込む処理をする。すなわち、定義ファイルのバージョンが改訂されている場合には、改訂前後の差分を取り込むこと、更新されたファイル全体を取り込むこと等により、ウィルス定義ファイルを更新する。その後は、同様の処理を自動的に周期的に繰り返す。例えば、特許文献１（特開２００２－２５９１５０号公報）には、こうしたウィルス定義ファイルの更新技術が紹介されている。

ところで、上記のような従来の技術には、次のような解決すべき課題があった。

コンピュータの使い方として、ローカルで使用する場合、すなわち、ネットワークに接続せずに単独で使用する場合がある。また、ネットワークに接続される前に起動して、ローカルで使用されることがある。例

えば、モバイルコンピュータのように、ユーザが持ち歩くようなコンピュータの場合、ネットワークに接続しない状態での使用が行われることが多い。

ところで、ウィルス対策ソフトウェアは、コンピュータの起動時に、起動されて、周期的に定義ファイルの修正分取り込み処理を試みる。しかし、当該コンピュータが、ネットワークに接続されていない場合には、ファイルの更新に失敗することになる。また、コンピュータをネットワークに接続しない状態が続くと、長期間定義ファイルの修正分取り込み処理がなされないままになっていることが起きる。こうしたコンピュータを、起動させたままの状態で、ネットワークに接続すると、ウィルス対策ソフトウェアが次のタイミングで定義ファイルの修正分取り込み処理を実行するまでは、新種のウィルスに対し、無防備な状態になる。

発明の開示

本発明は、特定のプログラムの起動時に、特定のデータを、ネットワークを介して取得する技術を提供することを目的とする。

本発明の第１の態様によれば、

ネットワークを介してコンピュータが特定のデータを取得する方法において、

特定のプログラムについての起動指示の検知を行い、

特定のプログラムについての起動指示を検知すると、ネットワークを介して特定のデータを取得するための特定データの取得処理を行い、

その後、前記起動が指示された特定のプログラムの起動を行うことを特徴とする、特定のデータを取得する方法が提供される。

本発明の第２の態様によれば、

ネットワークを介して特定のデータを取得するシステムにおいて、

特定のプログラムについての起動指示の検知を行う手段と、

特定のプログラムについての起動指示を検知すると、ネットワークを

介して特定のデータを取得するための特定データの取得処理を行う手段と、

特定データの取得処理後、前記起動が指示された特定のプログラムの起動を行う手段と、を備えること

を特徴とする、ネットワークを介して特定のデータを取得するシステムが提供される。

本発明の第３の態様によれば、

コンピュータのネットワークセキュリティ強化システムにおいて、

ネットワークに接続をして通信を実行するプログラムの起動時に、前記ネットワークへの接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システムが提供される。

本発明の第４の態様によれば、

コンピュータのネットワークセキュリティ強化システムにおいて、

コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

ネットワーク接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、

その後、前記通信を実行するプログラムを起動する、制御プログラムを、自動的に生成する手段を備えたことを特徴とするネットワークセキュリティ強化システムが提供される。

本発明の第５の態様によれば、

ネットワークに接続をして通信を実行するプログラムの起動時に、ネットワーク接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させるように、コンピュータを動作させることを特徴とするネットワークセキュリティ強化プログラムが提供される。

更に、本発明の第６の態様によれば、

コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

前記ネットワークへの接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動する制御プログラムを、自動的に生成する処理を、コンピュータに実行させることを特徴とするネットワークセキュリティ強化プログラムが提供される。

図面の簡単な説明

図１は、ネットワークセキュリティ強化システムの具体例を示すブロック図である。

図２は、ネットワークセキュリティ強化システムの別の具体例を示すブロック図である。

図３（ａ）から図３（ｄ）は、図１に示したネットワークセキュリティ強化システムの動作中に表示される画面例を示す説明図である。

図４（ａ）および図４（ｂ）は、ネットワーク接続制御プログラムをインストールする際の設定操作の画面例を示す説明図である。

図５（ａ）および図５（ｂ）は、ネットワーク接続制御プログラムの動作フローチャートである。

図６（ａ）および図６（ｂ）は、ネットワーク接続制御プログラムの別の動作フローチャートである。

図７は、通信を行うプログラムの起動時に、特定のデータを取得する方法の動作の概要を示す説明図である。

図８は、ネットワーク接続制御プログラムの機能構成を示す説明図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について、図面を参照して説明する。まず、特定のプログラムの起動時に、ネットワークを介して特定のデータを取得する方法に関する実施形態について、図７を参照して説明する。

本実施形態では、特定のプログラムについての起動指示をトリガーとして、コンピュータが、他の処理に先立って、予め定められた他のコンピュータ、例えば、特定のサーバから、特定のデータを取得する処理を行う。そのために、コンピュータは、特定のプログラムの起動指示を検知する処理１１１を行う。すなわち、コンピュータは、特定のプログラムの起動指示を検知する処理１１１において、特定のプログラムについての起動指示の検知を行い、かつ、起動指示が検知されると、その後の一連の処理を行うためのシーケンスを起動する。このシーケンスに従って、コンピュータは、ネットワーク接続処理１１３を行い、さらに、ネットワークを介して特定のデータを取得するための特定データ取得処理１１４を行う。その後、起動することが指示された、特定のプログラムの起動１１６を行う。

この結果、特定のプログラムの起動指示を検知する処理１１１が行われた時点では、当該起動が指示された特定のプログラムの起動は行われない。すなわち、特定のデータの取得処理が、起動が指示された特定のプログラムの起動処理に先行して行われる。

ここで、起動指示の検知の対象となる特定のプログラムは、予め定められたプログラム、または、ユーザにより指定されたプログラムである。例えば、通信を行うプログラムが挙げられる。より具体的には、図１、図２に示されるような、メーラーと称されるメール管理プログラム１３、ブラウザ１４、ダイヤルアッププログラム１５等が挙げられる。特定のプログラムは、システムにおいて予め指定する構成とすることができる。また、ユーザにおいて、全部または一部を指定する構成としてもよい。さらに、追加、削除等の指定の変更がユーザにより行えるように

してもよい。特定のプログラムの指定については後述する（図４（ａ）参照）。

また、特定のプログラムの起動指示は、入力装置を介してユーザから行われる場合に限られない。例えば、アプリケーションプログラム等において起動が指示される場合が含まれる。

特定のデータは、特定のプログラムの起動に先行して取得すべきものとして、予め定められたデータである。例えば、ウィルス対策ソフトウェアの更新処理を行うためのデータ、アプリケーションプログラムのアップグレード用データ等が挙げられる。ウィルス対策ソフトウェアの更新処理を行うためのデータとして、より具体的には、ウィルス定義ファイル、パッチファイル等が挙げられる。このようなセキュリティ対策用のソフトウェアを、コンピュータのネットワーク接続時に取得し、更新処理することにより、そのコンピュータについてネットワークセキュリティの強化を図ることができる。

ここで、セキュリティ対策用ファイルの更新処理とは、コンピュータをネットワークに接続した場合のセキュリティ対策用のためのソフトウェアを、ネットワークを通じて取得して更新する処理を意味する。具体的な更新処理としては、ウィルス対策用のウィルス定義ファイルの修正分取り込み処理、パッチファイルの取り込み処理等が挙げられる。修正分は、差分データの形式である場合、修正して更新されたデータファイルの形式である場合等、種々の形式での供給があり得る。

この処理は、望ましい態様としては、通信を実行するプログラムの起動時に実行される。しかも、ネットワーク接続処理後、他の処理に先行して行われる。その結果、通信を実行するプログラムの動作開始前に最新のセキュリティ対策が施される。ネットワークへの接続が長時間に及ぶ場合は、その後、一定時間おきに、セキュリティ対策用ファイルの更新処理を起動することが好ましい。

前述した特定のプログラムについての起動指示の検知については、コンピュータがネットワークに接続されて、最初に行われる、特定のプロ

グラムについての起動指示のみを検知するようにしてもよい。そのため、最初の起動指示を検知するための最初の起動指示検知処理１１２（図７、図５（ｂ）参照）を付加することができる。

このように、特定のプログラムについての起動指示検知を、初回のみ行う構成とすることにより、その後、特定のプログラムの再立ち上げ、追加立ち上げ等を行っても、特定のデータ取得処理を回避することができる。これにより、特定のプログラムの立ち上げ処理が速くなる。

なお、ネットワークセキュリティ対策ファイルの取得の場合、ネットワーク接続後は、ウィルス対策プログラムにより、ウィルス対策ファイルの修正分等の収録を定期的に行わせることができる。従って、その場合には、起動時を除いて、本発明を利用したネットワークセキュリティ強化を動作させなくてもよい。

また、特定データ取得処理１１４を行った後、取得処理の結果を示すメッセージを、コンピュータの表示装置に表示させるメッセージ表示処理１１５を付加することができる。取得処理の結果を示すメッセージとしては、例えば、特定データの取得処理について、取得できたこと、取得できなかったこと、取得の必要がなかったこと等を示すメッセージが挙げられる。具体的には、ウィルス対策ファイルの取得処理を終了した後に、当該更新がされたことを報告するメッセージを表示装置に表示させる。これにより、ウィルス対策ファイルの更新処理が行われたことをユーザに知らせることができる。従って、ユーザは、安心して、コンピュータをネットワークに接続した状態で利用できる。また、動作エラー等により、ウィルス対策ファイルの更新処理ができなかった旨のメッセージが表示されることにより、コンピュータが無防備な状態にあることが、ユーザに報知される。従って、ユーザは、コンピュータをネットワークから切断する等の対策を行うことができる。

前述した各種処理１１１から１１６は、後述する図１または図２に示すコンピュータ１０により実現される。より具体的には、コンピュータ１０が有する演算処理装置１００が対応するプログラムを実行すること

により、実現される。演算処理装置１００には、各種プログラムがロードされ、それぞれの機能が実現される。

このような処理機能をコンピュータにより実現させるためのプログラムとして、本発明の実施形態においては、ネットワーク接続制御プログラム１７、ネットワーク接続のためのプログラム、ネットワークを介して特定のデータを取得するためのプログラム等が用いられる。これらのプログラムをコンピュータ１０の演算処理装置１００が実行することにより、特定のデータを取得するシステムが構築され、特定のデータを取得する方法が実現される。

図８に、ネットワーク制御プログラム１７を構成する複数のプログラムの一例を示す。図８に示すプログラムは、これまでに説明した機能を実現するものの他、ネットワーク制御プログラム１７自体を、自動的にプログラミングする機能をも含む。

すなわち、ネットワーク制御プログラム１７は、特定のプログラムの起動指示検知１７１と、最初の起動指示検知処理１７２と、ネットワーク接続指示１７３と、特定データの取得指示１７４と、メッセージ表示処理１７５と、特定のプログラム起動処理１７６と、プログラム自動生成処理１７７とを有する。

ここで、特定のプログラムの起動指示検知１７１は、特定のプログラムの起動１７６に対する起動指示を検知するものである。例えば、後述する図１、図２に示す例では、特定のプログラムとして、メーラー１３、ブラウザ１４、ダイヤルアッププログラム１５等に対する起動指示を検知するものである。この特定のプログラムの起動指示検知１７１を実行することにより、図７に示す前述した特定のプログラムの起動指示検知１１１を実現する。

また、この特定のプログラム起動指示検知１７１は、起動指示を検知すると、その後の一連の処理を行うシーケンスを起動する。すなわち、最初の起動指示検知処理１７２と、ネットワーク接続指示１７３と、特定データの取得指示１７４と、メッセージ表示処理１７５と、特定のプ

ログラム起動処理１７６とを順次行うシーケンスを起動する。

このネットワーク接続制御プログラム１７を、ネットワークセキュリティ強化のために適用した例が、図１、図２に示すネットワークセキュリティ強化システムである。また、ネットワーク接続制御プログラム１７の処理の流れは、例えば、図５および図６に示すように行われる。

このように、本発明によれば、ネットワークに接続して通信を実行するプログラム等の、特定のプログラムの起動時に、前記ネットワークへの接続処理後、他の処理に先行して、特定のデータとして、セキュリティ対策用ファイルを取得する、ネットワークセキュリティ強化のための方法、および、それを実現するためのシステムが提供できる。

次に、本発明をコンピュータのネットワークセキュリティ強化に適用した場合における実施の形態について説明する。

図１は、ネットワークセキュリティ強化システムの具体例を示すブロック図である。図１に示すように、セキュリティ強化の対象になっているコンピュータ１０は、ネットワークインタフェース１１を介してネットワーク１に接続される。

ネットワーク１には、ウィルス対策プログラムの提供元のサーバ２０が接続されている。このサーバ２０には記憶装置２１が設けられている。サーバ２０は、定義ファイル２２を、ネットワーク１を通じてユーザのコンピュータ１０に提供する。

コンピュータ１０には、記憶装置１２と演算処理装置１００が設けられている。また、コンピュータ１０には、表示装置１０ａと入力装置１０ｂとが設けられている。入力装置１０ｂには、キーボード、マウス等が含まれる。

演算処理装置１００には、メーラー（メール管理プログラム）１３と、ブラウザ１４と、ダイヤルアッププログラム１５と、ウィルス対策プログラム１６と、ネットワーク接続制御プログラム１７とがロードされている。ここでは、本発明の説明に関係するプログラムの存在を示している。もちろん、演算処理装置１００において実行されるプログラムは

、これらに限定されるものではない。演算処理装置１００において実行されるプログラムは、記憶装置１２に格納され、演算処理装置１００にロードされる。

メーラー（メール管理プログラム）１３は、メールの送受信を制御するプログラムである。ブラウザ１４は、インターネット閲覧用のプログラムである。ダイヤルアッププログラム１５は、あらかじめ設定された電話番号に対してダイヤルアップ接続をする制御を行うプログラムである。

ウィルス対策プログラム１６は、ウィルスチェックを実行するプログラムである。ウィルス対策プログラム１６が動作するためには定義ファイル２２が必要になる。ウィルス対策プログラム１６の提供元は、新たなウィルスが発生するたびに定義ファイル２２の修正分ファイルを提供する。

このため、ウィルス対策プログラム１６は、特定のデータを取得するためのプログラムとして、ウィルス定義ファイル修正分を取り込むための定義ファイル修正分取り込みプログラム１８を備える。ウィルス対策プログラム１６は、あらかじめ設定された時間間隔で周期的に定義ファイル修正分取り込みプログラム１８を起動する。

定義ファイル修正分取り込みプログラム１８は、所定のタイミングで定期的にサーバ２０から定義ファイル２２をダウンロードし、記憶装置１２に記憶させる機能を持つ。すなわち、記憶装置１２に記憶される定義ファイル２２を更新処理する。

ネットワーク接続制御プログラム１７は、メーラー（メール管理プログラム）１３、ブラウザ１４等を利用するために、ユーザがいずれかを起動すると、まず、ダイヤルアッププログラム１５を起動し、次にウィルス対策プログラム１６の定義ファイル修正分取り込みプログラム１８を起動する。こうして、通信用のプログラムを実行する前に、まず、定義ファイル２２を最新のものに更新しておく機能を持つ。この発明では、メーラー１３、ブラウザ１４、ダイヤルアッププログラム１５など、

ネットワークに接続をして通信を実行するプログラムの起動時に、自動的にウィルス対策ソフトによる定義ファイルの修正分取り込み処理を実行させる。これによって、常に最新の定義ファイルを利用し、例えば、モバイルコンピュータがネットワークを通じて安全に通信をすることができる。なお、通信を実行するプログラムの起動は、ユーザによって、直接、起動が指示される場合のみならず、アプリケーションを介して起動指示される場合も含む。

なお、図１および図２に示す例では、ネットワーク接続制御プログラム１７は、図８に示す各種機能のうち、特定のプログラムの起動指示検知１７１、ネットワーク接続指示１７３、特定データの取得指示１７４、メッセージ表示処理１７５、および、起動することが指示された特定のプログラム起動指示１７６を実行するための機能を備えている。

図２は、ネットワークセキュリティ強化システムの別の具体例を示すブロック図である。図２に示す例を、図１に示す例と比較して説明する。

コンピュータ１０には、ウィルス対策プログラム１６の代わりに、パッチファイル取り込みプログラム１９が設けられている。なお、１台のコンピュータにウィルス対策プログラム１６とパッチファイル取り込みプログラム１９とを併せて備えることが好ましい。しかし、本明細書では、説明の都合上それぞれ独立に実例を示した。

ネットワーク接続制御プログラム１７は、ダイヤルアッププログラム１５を起動した後に、パッチファイル取り込みプログラム１９を起動するように動作する。ネットワーク１にはサーバ２５が接続されている。このサーバ２５は、例えば、メーラー（メール管理プログラム）１３、ブラウザ１４等を提供する提供元が管理する。サーバ２５に設けられた記憶装置２６には、メーラー（メール管理プログラム）１３、ブラウザ１４のセキュリティ改善のためのパッチファイル２３が記憶されている。パッチファイル取り込みプログラム１９は、ネットワーク１を通じてパッチファイル２３をダウンロードし記憶装置１２に記憶する機能を持

つ。このパッチファイル２３によってメーラー（メール管理プログラム）１３、ブラウザ１４等がその都度更新される。

図３（ａ）から図３（ｄ）は、図１に示したネットワーク接続制御プログラム１７の動作中に表示される画面例の説明図である。

既に説明したように、コンピュータ１０は、ネットワーク接続制御プログラム１７として、図８に示すように、各種機能１７１から１７６を備えている。例えば、メーラー１３の起動が指示されると、演算処理装置１００は、メーラー１３の起動指示を検知すると共に、ダイヤルアッププログラム１５を起動させる処理をする。その結果、ネットワークの接続条件の設定が行われる。続いて、演算処理装置１００は、ウィルス対策プログラム１６の定義ファイル修正分取り込みプログラム１８を起動して、定義ファイルの修正分取り込み処理を実行させる。

このとき、演算処理装置１００は、メッセージ表示処理１７５を実行して、その処理が完了したことをユーザに伝えるために、図３（ａ）の画面３１を表示装置１０ａに表示する。ここでは、ユーザに対し、「ウィルス定義ファイルの更新をしました」というメッセージを表示する。これにより、安心してメーラー（メール管理プログラム）１３を利用できることが、ユーザに伝えられる。

演算処理装置１００は、ユーザによるボタン４１のクリックに基づいて、この画面３１を閉じる。その後、メーラー（メール管理プログラム）１３を起動して、通常通り、メールの送受信を可能とする。

なお、一般に、ブラウザは、画面を表示すると、既にネットワークを通じて初期画面のダウンロードを開始する。従って、ブラウザの画面表示より前に、定義ファイル２２の更新処理、ブラウザのパッチファイルを当てる処理等を実行しておくことが好ましい。

ウィルス定義ファイルの修正分取り込み処理は、既知の方法でよい。例えば、ＸＭＬデータベース形式でサーバからダウンロードして、アップデートすればよい。また、アプリケーションプログラムのセキュリティホール修復の目的で、アプリケーションプログラム供給元から配布さ

れる。パッチファイル２３の取得とパッチを当てる処理についても、同様の手順で実行できる。図３（ｂ）は、パッチファイル２３の取得とパッチを当てる処理の場合の、表示画面３２の例である。

前述した例では、定義ファイル２２およびパッチファイル２３を、演算処理装置１００が自動的に取得する処理を行っている。しかし、本発発明はそれに限られない。例えば、定義ファイル２２、パッチファイル２３等の更新処理を実行する前に、ユーザの了解をとる構成とすることができる。この場合には、図３（ｃ）に示す画面３３のように、「インターネット接続前にウィルス定義ファイルの更新をします」といったメッセージを、表示装置１０ａに表示する。

演算処理装置１００は、ボタン４３のクリックを、入力装置１０ｂを介して受け付けると、ユーザの了解が得られた状態と判断して、定義ファイル更新分取り込みプログラム１８を起動する。パッチファイル取り込みプログラム１９の起動についても同様の制御が可能である。

このほかに、定義ファイル２２やパッチファイル２３の更新処理をユーザの操作により実行する構成とこともできる。演算処理装置１００は、図３（ｄ）に示す画面３４のように、ネットワークの接続条件設定直後に、「メール送受信の開始前にセキュリティ対策ファイルの更新をして下さい」といったメッセージを表示する。演算処理装置１００は、この画面で、ボタン４４のクリックを、入力装置１０ｂを介して受け付けると、定義ファイル２２の更新処理を実行する。また、ボタン４５のクリックを、入力装置１０ｂを介して受け付けると、パッチファイル２３の更新処理を実行する。

具体的には、メーラー１３、ブラウザ１４、ダイヤルアッププログラム１５などの立ち上げ時の画面に、「定義ファイルの更新をして下さい」というメッセージが表示出力される。メッセージは、音声で出力される構成としてもよい。セキュリティ対策用ファイルの更新処理は、通信を実行するプログラムと連動していなくて構わない。この場合には、無用なファイル更新処理を回避することができる。

また、ブラウザ１４の起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する構成としてもよい。この場合、ブラウザ１４の起動時に、「定義ファイルやパッチファイルの更新をして下さい」というメッセージが表示出力される。従って、自動化はされないが、セキュリティは確保される。

図４は、ネットワーク接続制御プログラム１７をインストールしたときの動作説明図である。ネットワーク接続制御プログラム１７は、多数のコンピュータにインストールされて、その機種を選ばずに動作するように、以下の機能を持つことが好ましい。

図４（ａ）の画面３５に示すように、初めに、インストールされるべきコンピュータの通信用ソフトを検索する。そして、制御対象になるソフトウェアを決定する。画面３５には、リストボックス３７とボタン４６～５０とが設けられている。インストール直後、演算処理装置１００は、リストボックス３７に当該コンピュータ中に用意されている通信用ソフトウェアのリストを表示する。ユーザがこの中から普段使用しているメーラーとブラウザとを残して、不要なものを選択して、削除ボタン４８をクリックすると、演算処理装置１００は、削除指示されたソフトウェアを削除する。一方、他にも通信用ソフトウェアがある場合には、追加ボタン４６が押されることを検知して、演算処理装置１００は、追加する処理を行う。参照ボタン４７がクリックされると、演算処理装置１００は、参照対象をリストに表示する。

こうして、制御の対象となる通信用ソフトウェアを決定することができる。演算処理装置１００は、入力装置１０ｂを介して、ユーザによるＯＫボタン４９のクリックを受け付ける。また、演算処理装置１００は、入力装置１０ｂを介して、キャンセルボタン５０のクリックを受け付けて、すべての処理をキャンセルする。

以上の準備処理によって、演算処理装置１００は、ネットワーク接続制御プログラム１７により、図４（ｂ）に示すような起動画面を生成する。起動画面３８は、上記のようなネットワークセキュリティの強化を

図りながら、メールやインターネットを利用するための、新たなアプリケーションの画面である。この画面３８には、例えば「ネットワーク接続ユーティリティ」といった表題が付けられる。

演算処理装置１００は、入力装置１０ｂを介して、ボタン５１のクリックを受け付けると、メーラー１３を起動する。入力装置１０ｂを介して、ボタン５２のクリックを受け付けると、ブラウザ１４を起動する。ネットワーク制御プログラム１７には、図４（ｂ）に示すような画面３８を表示するフォームと、ボタン５１および５２のクリックイベントにより実行されるコマンドのリストとが含まれる。そのコマンドの意味は、画面３８の下側に示したとおりである。すなわち、例えば、「メールを送受信する」が選ばれた場合、〔ダイヤルアップ起動〕５１１、〔定義ファイル修正分取り込み〕５１２、〔メッセージ表示〕５１３および〔メーラー起動〕５１４を意味するコマンド群が含まれる。

図５（ａ）および図５（ｂ）は、ネットワーク接続制御プログラムの動作フローチャートである。ここで、図５（ａ）は、ネットワーク接続制御プログラム１７の具体的な動作フローチャートである。このネットワーク制御プログラム１７の動作は、前述した図８に示す機能１７１から１７６により実現される。

ステップＳ１で、演算処理装置１００は、特定のプログラムの起動指示検知機能１７１を実行して、図４（ｂ）に示した画面３８を表示して、通信用プログラムの起動指示を待つ。演算処理装置１００は、この画面において、入力装置１０ｂを介してボタン５１がクリックされてメーラー１３の起動が指示された場合には、指定された特定のプログラムに相当する通信用プログラムの起動指示と判断して、ステップＳ１からステップＳ２へ進む。ステップＳ２では、制御シーケンスを起動する。制御シーケンスとは、ステップＳ３からステップＳ７の、一連の処理のことである。

次に、ステップＳ３で、演算処理装置１００は、ネットワーク接続指示機能１７３を実行し、ダイヤルアッププログラム１５を起動する。そ

して、ダイヤルアッププログラム１５を実行して、ステップＳ４で接続を確立させる。これにより、ネットワーク１との接続が可能となる。演算処理装置１００は、ステップＳ５で、特定データの取得指示機能１７４を実行し、定義ファイル修正分取り込みプログラム１８を起動する。演算処理装置１００は、定義ファイル修正分取り込みプログラム１８を実行して、サーバ２０から定義ファイル２２の修正分をダウンロードする。もちろん、併せて、パッチファイル２３のダウンロードを実行することもできる。

その後、ステップＳ６で、演算処理装置１００は、メッセージ表示処理機能１７５を実行して、処理完了メッセージを表示する。このメッセージは、例えば、表示装置１０ａに、前述した図３（ａ）に示すように表示される。

最後に、演算処理装置１００は、ステップＳ７で、通信用プログラムを起動して処理を終了する。すなわち、前述した特定のプログラムの起動指示検知機能１７１により検知された通信用プログラムであるメーラー１３を起動する。

図５（ｂ）は、制御プログラムのオプションとして設けられた、最初の起動指示検知処理１７２（図８参照）のプログラムによる処理の流れを示す。ネットワークに接続をして既に定義ファイル２２やパッチファイル２３の更新処理を済ませた後、いったん通信用プログラムも終了させることがある。この場合に、ネットワークの接続を継続していれば、定義ファイル修正分取り込みプログラム１８やパッチファイル取り込みプログラム１９はそのまま正常に動作している。従って、一定時間おきに定義ファイル２２やパッチファイル２３の更新処理が自動的に実行されている。その後、再び通信用プログラムを起動したときに、改めて起動時に定義ファイル２２やパッチファイル２３の更新処理を実行する必要はない。さもなければ、通信用プログラムの起動に時間がかかり操作性を悪くする。

そこで、最初の起動指示検知処理１７２では、図５（ｂ）のステップ

Ｓ２１で、ネットワーク接続中かどうかを判断する。ネットワークに接続中であれば、ステップＳ２２で、接続後に更新したかどうかを判断する。接続後に１回でも更新をした履歴が記録されていれば、ステップＳ２３で、制御プログラムの起動を中止する。もちろん、いったんネットワークを切断してしまった場合には、制御プログラムを起動させる。

次に、本発明の他の実施形態として、ネットワーク制御プログラム１７におけるプログラム自動生成処理１７７により、軌道制御プログラムを自動的に生成する例について説明する。このプログラム自動生成処理１７７は、コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、ネットワーク接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、上記通信を実行するプログラムを起動する、起動制御プログラムを自動的に生成するプログラムである。

上記軌道制御プログラムの自動生成を実現するには、ネットワーク接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動するという制御プログラムが必要である。しかしながら、コンピュータによって、インストールされている通信用のプログラムが異なる。そこで、あらかじめ、コンピュータにインストールされた、通信用のプログラムを検出し、自動的に起動制御プログラムを生成する手段を設けておく。これにより、各種の通信用プログラムをインストールした任意のコンピュータに対して、上記の機能を容易に付与できる。

図６（ａ）および図６（ｂ）は、ネットワーク接続制御プログラムの別の動作フローチャートである。図６（ａ）は、ネットワーク接続制御プログラム１７をインストールしたときの初期設定動作を示すフローチャートである。

まず、ステップＳ３１で、インストールを完了すると、演算処理装置１００は、ステップＳ３２で、通信用プログラムの検索をする。そして、ステップＳ３３で、通信用プログラムリストを生成する。ここで、そ

の結果を表示装置１０ａに表示する。ステップＳ３４で、追加要求があれば、ステップＳ３５でリストに対し通信用プログラムの追加処理を実行する。ステップＳ３６で、削除要求あれば、ステップＳ３７でリストの一部を削除処理する。最後に、ステップＳ３８で、起動制御プログラムの生成をする。

図６（ｂ）は、ネットワーク接続制御プログラム１７の起動制御をユーザに任せる場合のプログラムフローチャートである。すなわち、演算処理装置１００は、ステップＳ４１で、通信用プログラムの起動指示があると、ステップＳ４２で、制御プログラムの起動を要求する画面を、表示装置１０ａに表示する。入力装置１０ｂを介して、いずれかのボタンがクリックされると、該当するプログラムが起動する。この処理は、既に説明をしたとおりである。

上記のようにして、ネットワークに接続をして通信を実行するプログラムの起動時に、ネットワーク接続処理後他の処理に先行して、必ず、セキュリティ対策用ファイルの更新処理を起動させるようにしたので、例えば、長期間定義ファイルの更新をしないまま使用していたコンピュータを突然ネットワークに接続した場合でも、ウィルスの侵入から確実にコンピュータを防御できる。

なお、上記のコンピュータプログラムは、それぞれ独立したプログラムモジュールを組み合わせて構成してもよいし、全体を一体化したプログラムにより構成してもよい。コンピュータプログラムにより制御される処理の全部または一部を同等の機能を備えるハードウエアで構成しても構わない。また、上記のコンピュータプログラムは、既存のアプリケーションプログラムに組み込んで使用してもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えば、ＣＤ－ＲＯＭのようなコンピュータで読み取り可能な記録媒体に記録して、任意の情報処理装置にインストールして利用することができる。また、ネットワークを通じて任意のコンピュータのメモリ中にダウンロードして利用することもできる。

請求の範囲

１．　ネットワークを介してコンピュータが特定のデータを取得する方法において、

特定のプログラムについての起動指示の検知を行い、

特定のプログラムについての起動指示を検知すると、ネットワークを介して特定のデータを取得するための特定データの取得処理を行い、

その後、前記起動が指示された特定のプログラムの起動を行うことを特徴とする、特定のデータを取得する方法。

２．　請求項１に記載の方法において

前記特定プログラムについての起動指示は、通信を行うプログラムについての起動指示である、特定のデータを取得する方法。

３．　請求項２に記載の方法において、

前記特定データの取得処理は、セキュリティ対策用ファイルの更新処理である、特定のデータを取得する方法。

４．　請求項１および２のいずれか一項に記載の方法において、

前記起動が指示された特定のプログラムの起動は、前記起動指示された通信を行うプログラムの起動である、特定のデータを取得する方法。

５．　ネットワークを介して特定のデータを取得するシステムにおいて、

特定のプログラムについての起動指示の検知を行う手段と、

特定のプログラムについての起動指示を検知すると、ネットワークを介して特定のデータを取得するための特定データの取得処理を行う手段と、

特定データの取得処理後、前記起動が指示された特定のプログラムの

起動を行う手段と、を備えること
を特徴とする、ネットワークを介して特定のデータを取得するシステム。

６．　請求項５に記載のシステムにおいて
前記特定プログラムについての起動指示を行う手段は、通信を行うプログラムについての起動指示を行うものである、ネットワークを介して特定のデータを取得するシステム。

７．　コンピュータのネットワークセキュリティ強化システムにおいて、
ネットワークに接続をして通信を実行するプログラムの起動時に、前記ネットワークへの接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

８．　請求項７に記載のネットワークセキュリティ強化システムにおいて、
セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

９．　請求項７に記載のネットワークセキュリティ強化システムにおいて、
既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出する手段と、
当該プログラムの起動時の、ネットワーク接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段とを

備えたことを特徴とするネットワークセキュリティ強化システム。

１０．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理は、ウィルス対策用の定義ファイルの修正分取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

１１．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理は、パッチファイルの取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

１２．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

１３．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

ネットワークに接続をして通信を実行するプログラムによる、ネットワーク接続処理後、通信動作の開始前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

１４．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの

更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

１５．　コンピュータのネットワークセキュリティ強化システムにおいて、

コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

ネットワーク接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、

その後、前記通信を実行するプログラムを起動する、制御プログラムを、自動的に生成する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

１６．　ネットワークに接続をして通信を実行するプログラムの起動時に、ネットワーク接続処理後他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させるように、コンピュータを動作させることを特徴とするネットワークセキュリティ強化プログラム。

１７．　コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

前記ネットワークへの接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動する制御プログラムを、自動的に生成する処理を、コンピュータに実行させることを特徴とするネットワークセキュリティ強化プログラム。

図1

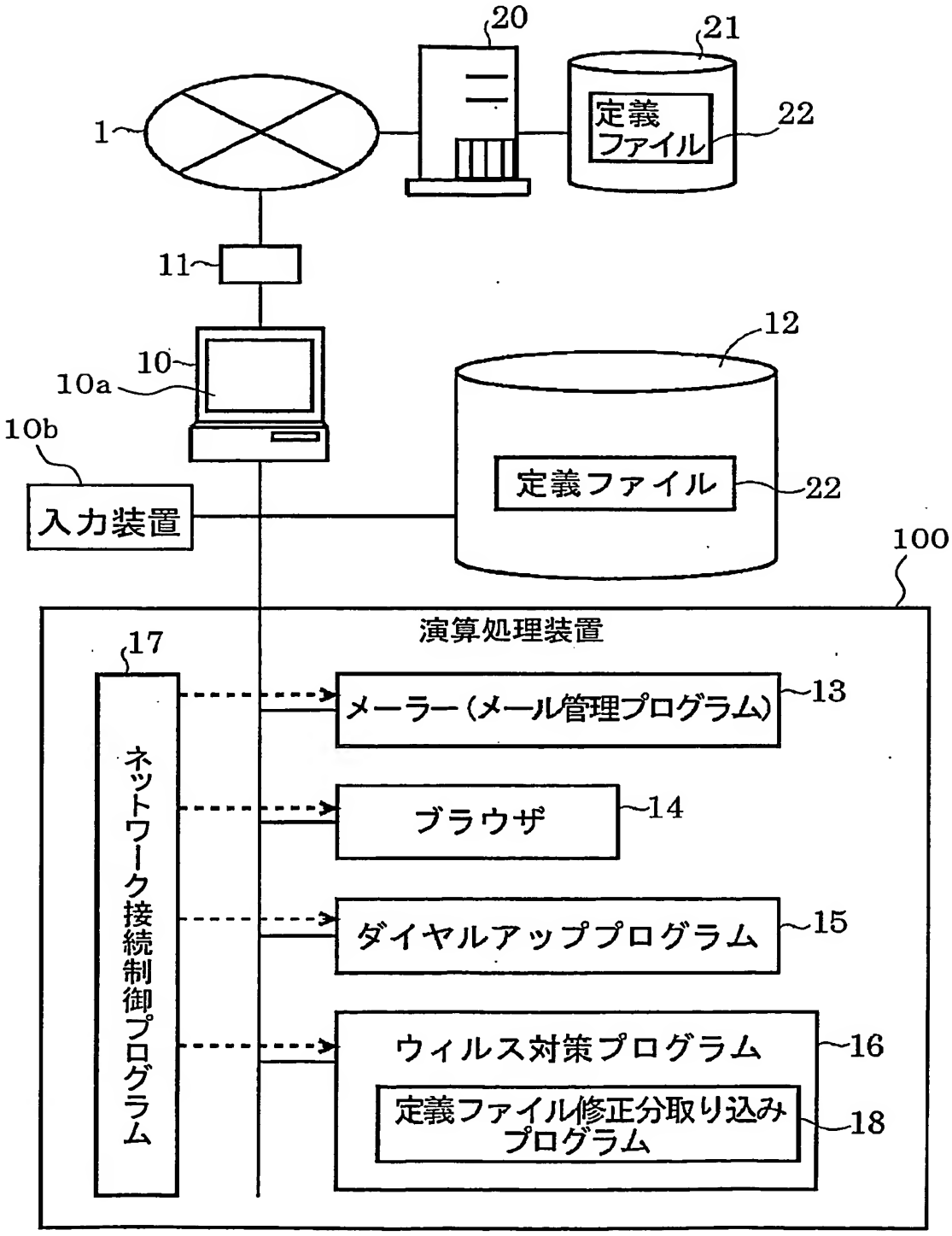

20
21
1
定義
ファイル
22
11
12
10
10a
10b
定義ファイル
22
入力装置
100
演算処理装置
17
メーラー(メール管理プログラム)
13
ネットワーク接続制御プログラム
ブラウザ
14
ダイヤルアッププログラム
15
ウィルス対策プログラム
16
定義ファイル修正分取り込み
プログラム
18

図2

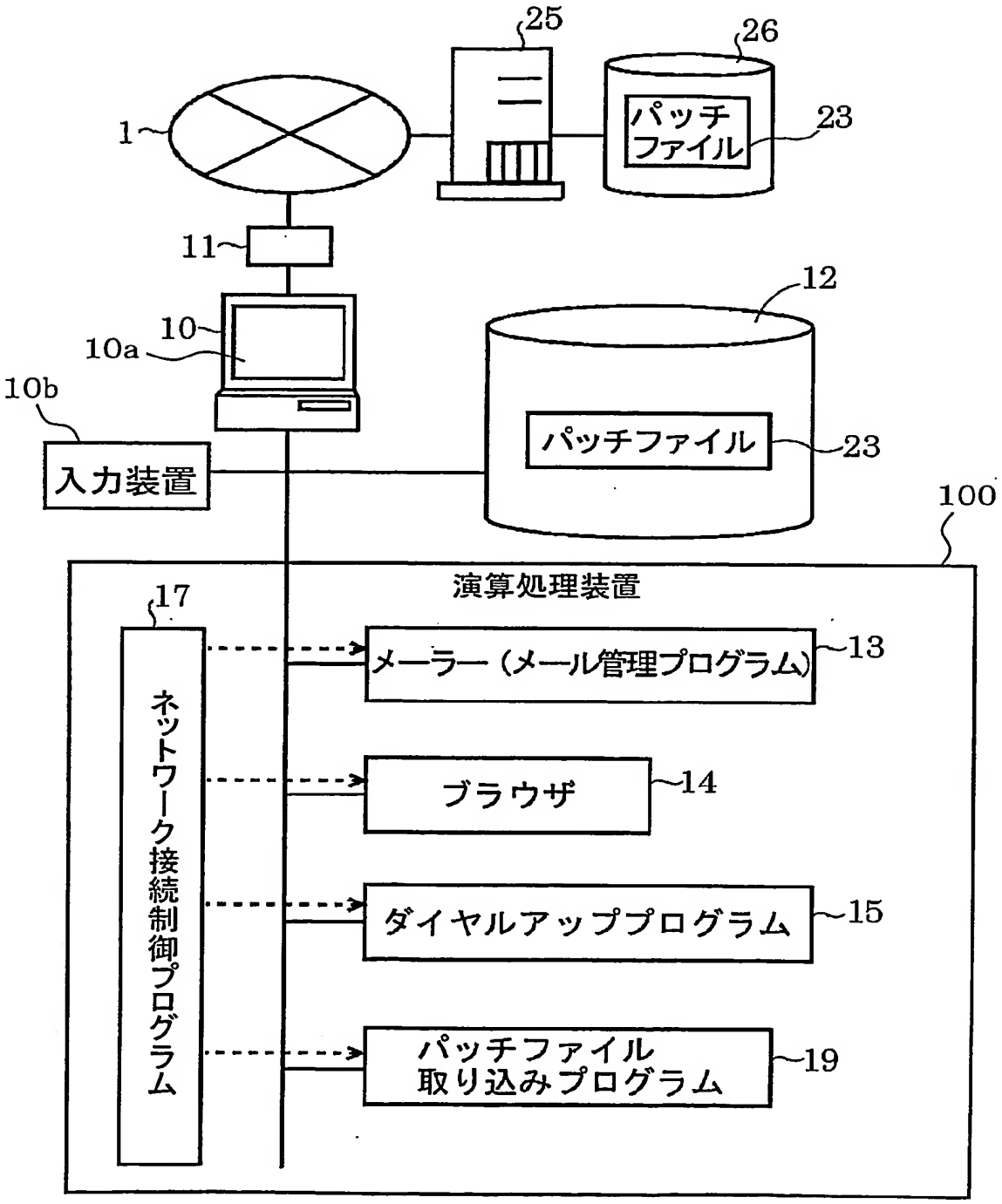
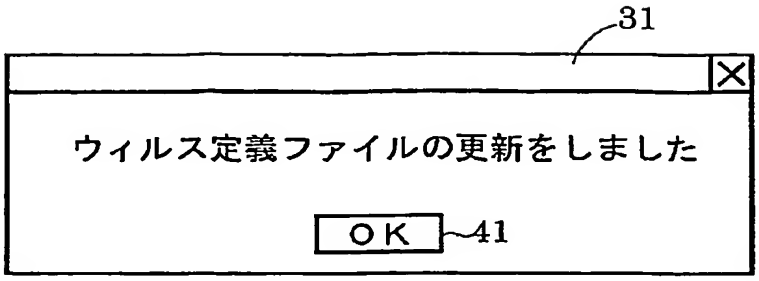
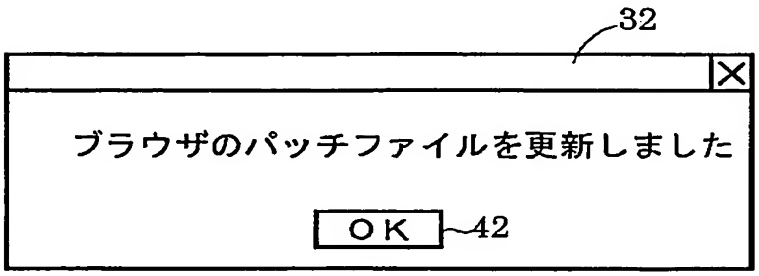

25
26
1
パッチファイル
23
11
12
10
10a
10b
パッチファイル
23
入力装置
100
演算処理装置
17
メーラー（メール管理プログラム）
13
ネットワーク接続制御プログラム
ブラウザ
14
ダイヤルアッププログラム
15
パッチファイル取り込みプログラム
19

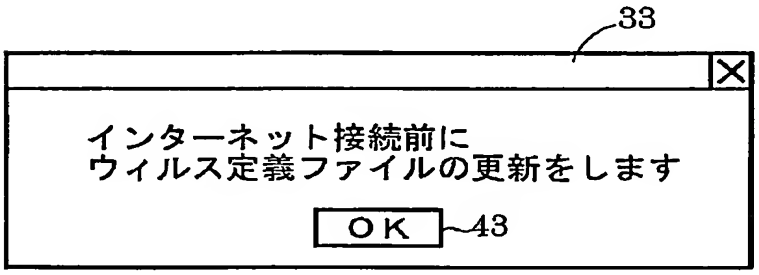
図3


31
ウィルス定義ファイルの更新をしました
OK
41

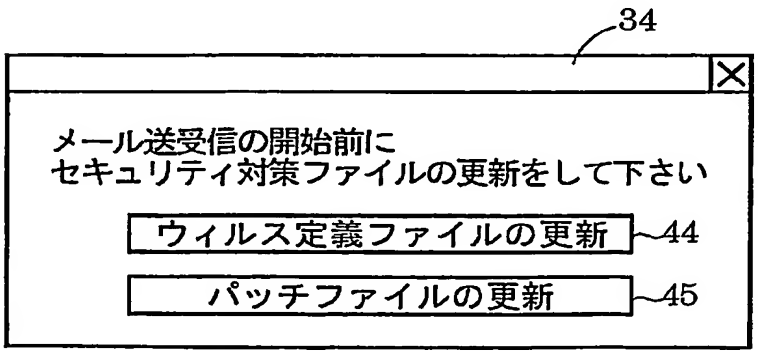
(a)


32
ブラウザのパッチファイルを更新しました
OK
42

(b)


33
インターネット接続前に
ウィルス定義ファイルの更新をします
OK
43

(c)


34
メール送受信の開始前に
セキュリティ対策ファイルの更新をして下さい
ウィルス定義ファイルの更新
44
パッチファイルの更新
45

(d)

図4

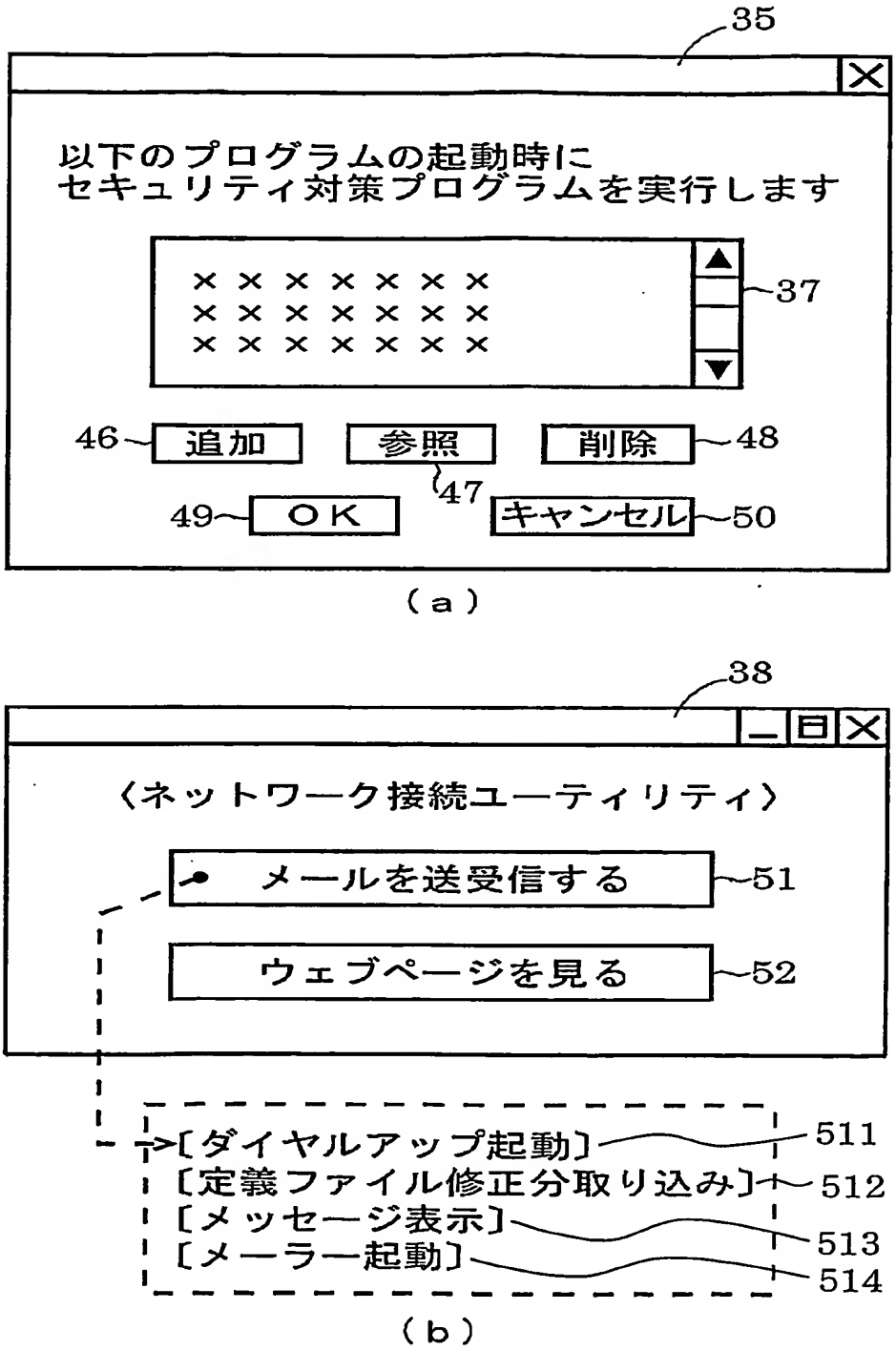

35
以下のプログラムの起動時に
セキュリティ対策プログラムを実行します
× × × × × × ×
× × × × × × ×
× × × × × × ×
37
46
追加
参照
削除
48
47
49
ＯＫ
キャンセル
50
（ａ）
38
〈ネットワーク接続ユーティリティ〉
メールを送受信する
51
ウェブページを見る
52
〔ダイヤルアップ起動〕
511
〔定義ファイル修正分取り込み〕
512
〔メッセージ表示〕
513
〔メーラー起動〕
514
（ｂ）

図5

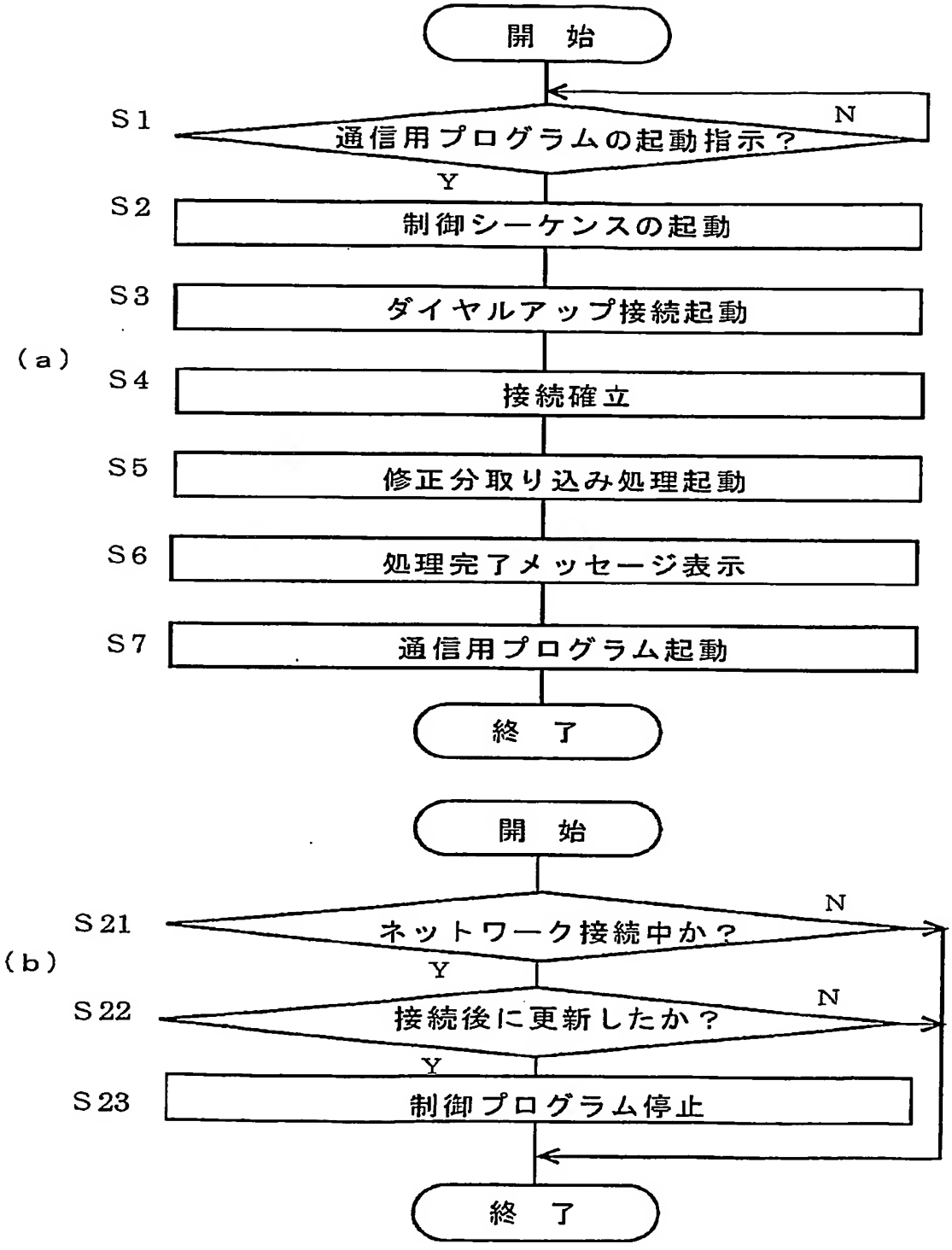

(a)
開　始
S1
通信用プログラムの起動指示？
N
Y
S2
制御シーケンスの起動
S3
ダイヤルアップ接続起動
S4
接続確立
S5
修正分取り込み処理起動
S6
処理完了メッセージ表示
S7
通信用プログラム起動
終　了
(b)
開　始
S21
ネットワーク接続中か？
N
Y
S22
接続後に更新したか？
N
Y
S23
制御プログラム停止
終　了

図6

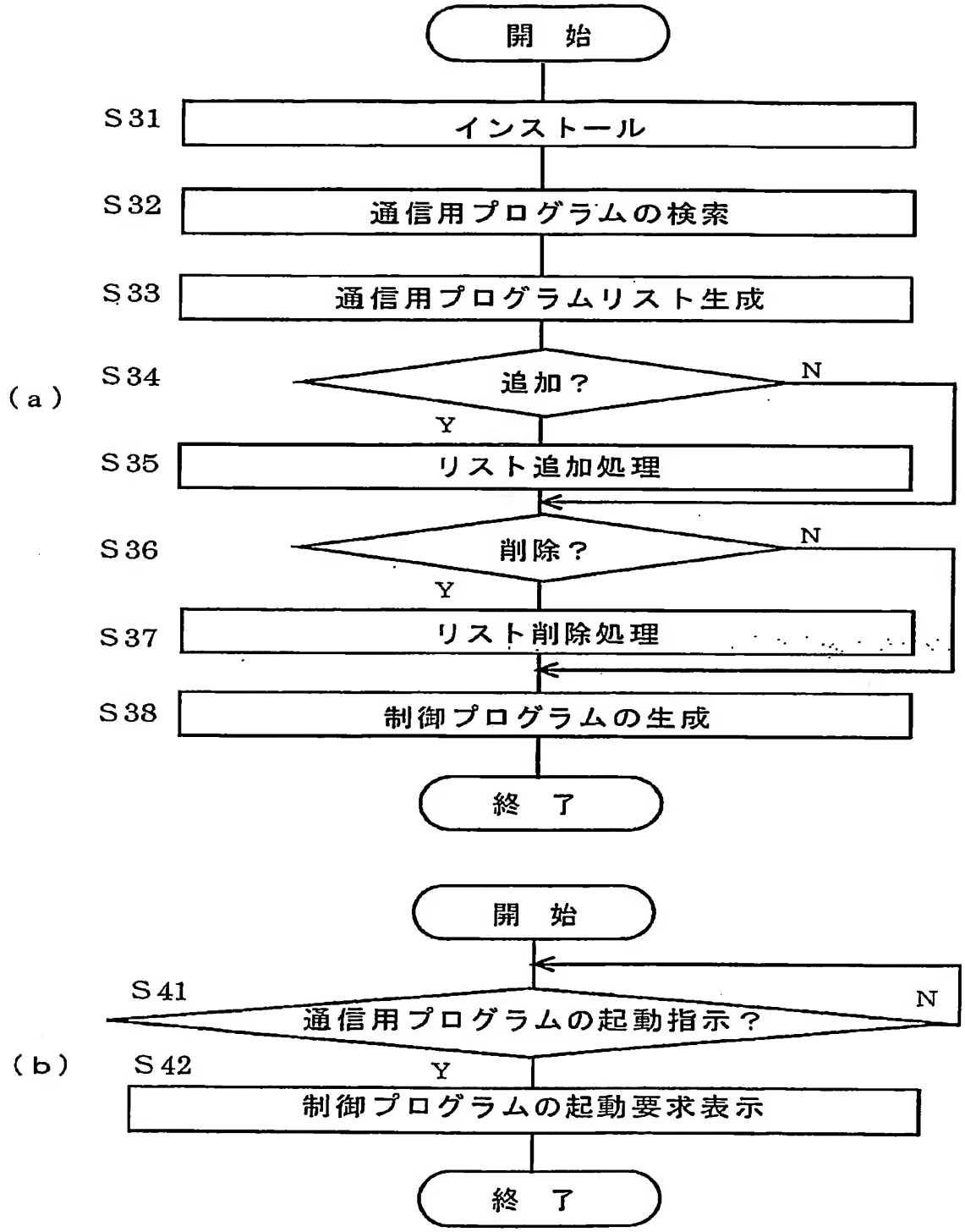

開　始
S31
インストール
S32
通信用プログラムの検索
S33
通信用プログラムリスト生成
S34
追加？
N
Y
S35
リスト追加処理
S36
削除？
N
Y
S37
リスト削除処理
S38
制御プログラムの生成
終　了
(a)
開　始
S41
通信用プログラムの起動指示？
N
Y
S42
制御プログラムの起動要求表示
終　了
(b)

図7

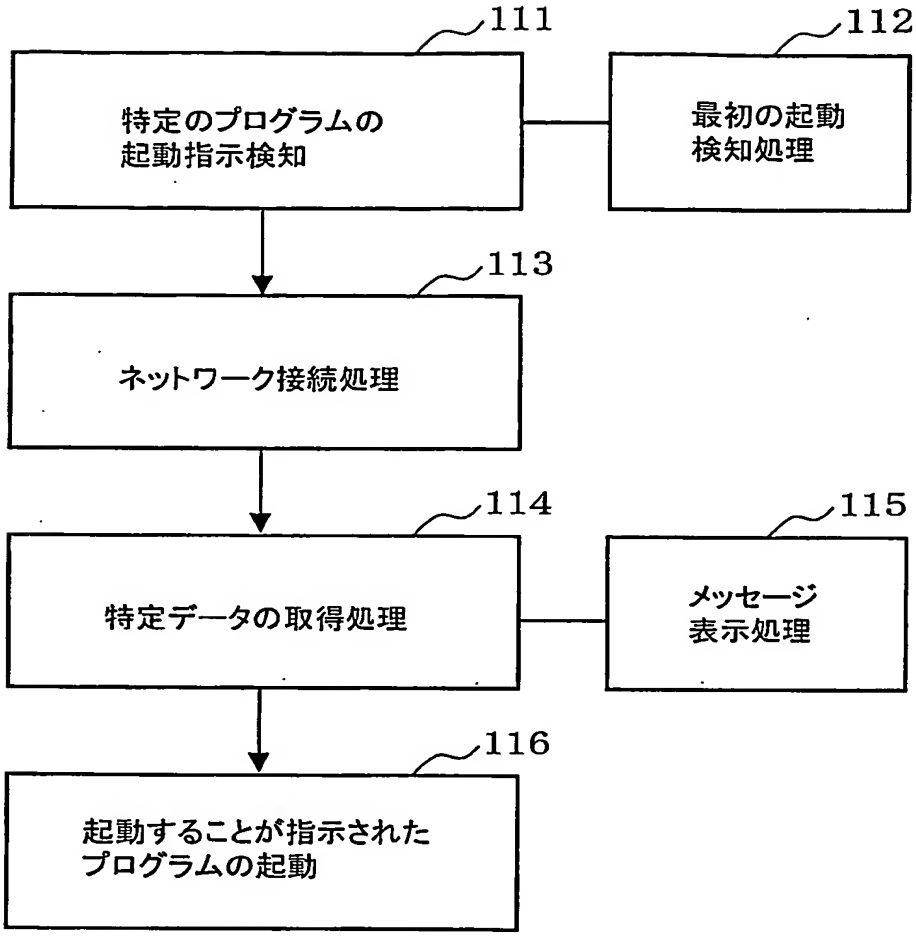
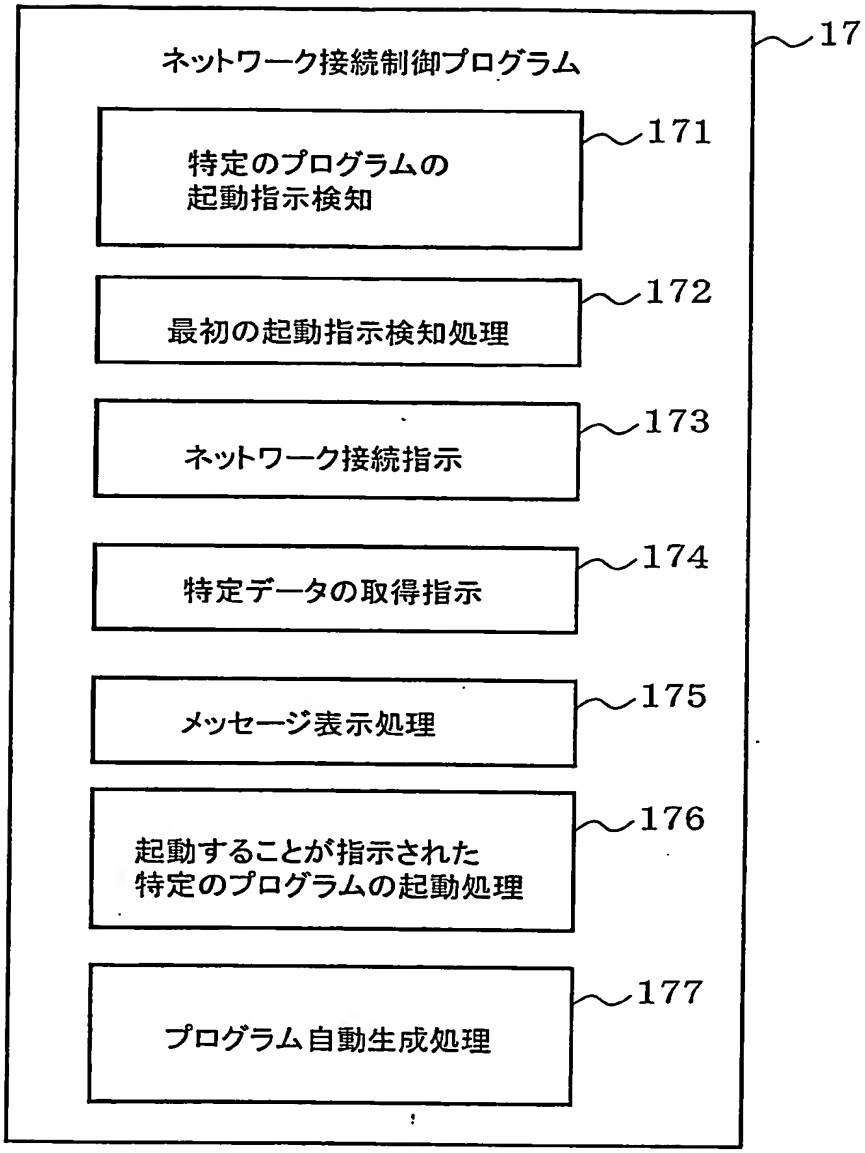

111
特定のプログラムの
起動指示検知
112
最初の起動
検知処理
113
ネットワーク接続処理
114
特定データの取得処理
115
メッセージ
表示処理
116
起動することが指示された
プログラムの起動

図8


17
ネットワーク接続制御プログラム
171
特定のプログラムの
起動指示検知
172
最初の起動指示検知処理
173
ネットワーク接続指示
174
特定データの取得指示
175
メッセージ表示処理
176
起動することが指示された
特定のプログラムの起動処理
177
プログラム自動生成処理

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/003533

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F11/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2002-287995 A (NTT Comware Corp.), 04 October, 2002 (04.10.02), Full text; all drawings (Family: none)	1-8,11-14,16 9,10,15,17
X A	JP 9-292980 A (NTT Data Communications Systems Corp.), 11 November, 1997 (11.11.97), Full text; all drawings (Family: none)	1-8,11-14,16 9,10,15,17
A	JP 2002-290900 A (Hitachi, Ltd.), 04 October, 2002 (04.10.02), Full text; all drawings (Family: none)	1-17

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 May, 2004 (26.05.04)	08 June, 2004 (08.06.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/003533

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-196942 A (Okiden Joho Service Kabushiki Kaisha), 12 July, 2002 (12.07.02), Full text; all drawings (Family: none)	1-17

国際調査報告

国際出願番号 PCT／JP2004／003533

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F11／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F11／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国実用新案登録公報	1996－2004年
日本国登録実用新案公報	1994－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X A	JP 2002－287995 A（エヌ・ティ・ティ・コムウェア株式会社）2002.10.04，全文，全図（ファミリーなし）	1-8, 11-14, 16 9, 10, 15, 17
X A	JP 9－292980 A（エヌ・ティ・ティ・データ通信株式会社）1997.11.11，全文，全図（ファミリーなし）	1-8, 11-14, 16 9, 10, 15, 17
A	JP 2002－290900 A（株式会社日立製作所）2002.10.04，全文，全図（ファミリーなし）	1-17

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 26.05.2004	国際調査報告の発送日 08.6.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 漆原 孝治　5B　9366 電話番号 03－3581－1101 内線 3546

様式PCT／ISA／210（第2ページ）（2004年1月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００３５３３

Ｃ．（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００２－１９６９４２　Ａ（沖電情報サービス株式会社）２００２．０７．１２，全文，全図（ファミリーなし）	1-17